INTERNATIONAL MARITIME ORGANIZATION

IMO

E

MARITIME SAFETY COMMITTEE
75th session
Agenda item 17

MSC 75/17/32
12 April 2002
Original: ENGLISH

PREVENTION AND SUPPRESSION OF ACTS OF TERRORISM AGAINST SHIPPING

Container security

Submitted by the United States

SUMMARY	
Executive summary:	This document provides the United States proposals for improving container security
Action to be taken:	Paragraphs 8, 9, 10, 11, 12 and 13
Related documents:	MSC 75/17/1

1 The intersessional meeting of the MSC Working Group on Maritime Security (ISWG) which met from 11-15 February 2002 considered a comprehensive set of proposals to improve maritime security submitted by the United States. One of these proposals was to address the issue of container security, taking into account technological advances in portable detection equipment and electronic sealing. Another was that IMO should work together with the World Customs Organization (WCO) with the aim of establishing international measures that would enhance the integrity of all cargo. The ISWG took note of a submission by ISO which informed the working group of an international pilot effort in containerized cargo identification and tracking using electronic seals.

2 The ISWG agreed to:

1. the need to maximize cooperation between all parties involved in the transport chain;
2. encourage targeting through information exchange;
3. the need to strike a balance between facilitation of maritime traffic and maritime security requirements;
4. recommend that the IMO Secretariat to commence or improve cooperation with other relevant organizations involved without delay;
5. recommend also the formalization of a cooperation agreement with the WCO;
6. encourage further discussion on this topic at MSC 75; and
7. urge delegates and observers to submit substantive documents to MSC 75.

3 During the discussion on container security at the ISWG, the United States identified a number of issues that should be further explored with the aim of improving maritime security from the cargo perspective. These included sealing of containers, non-intrusive detection and inspection, trusted agents and shippers, shipper identification numbers and cargo information in electronic format. The following is a discussion of each of these issues and a proposed course of action to address each of them taking into account the agreements at the ISWG meeting.

4 Sealing of containers. Currently, maritime containers conforming to ISO standards have two interlocking rear doors with a hasp capable of accepting a security seal. However, these containers are generally not required to be sealed, either mechanically or electronically. A fundamental of container security is to ensure that once a container is loaded and offered for shipment, it is secure from illegal intrusion for the purpose of smuggling contraband of any kind, but especially that which threatens maritime security. Container seals are widely used as a form of control to indicate that the cargo consigned is untouched en route. While a vast majority of containers are affixed with some type of seal, there is no universal standard or requirement for container seals, either mechanically or electronically. The potential risk posed by thousands of unsealed containers entering a country on a daily basis demands that consideration be given to a requirement calling for all containers to be sealed. A uniquely numbered container seal, together with the container identification number recorded on the shipping documents offer a necessary first step to improving container security. This information, in combination with the ability to verify if the seal is intact enables the appropriate authorities to easily and quickly determine if a container seal has been violated.

5 The U.S. recognizes that the ultimate end state for container seals are active electronic seals capable of storing and transmitting sufficient amounts of data for all shipping needs that will be developed through incremental steps brought about by advances in technology. All container seals, either electronic or mechanical, must provide the necessary level of security while allowing for smooth facilitation of commerce.

6 Immediate sealing of containers can be accomplished with uniquely numbered, mechanical (non-electronic), tamper proof manual seals designed in such a way that they must be destroyed to be removed. However, ISO is currently developing a standard for an electronic seal that stores and provides for remote access of information crucial to enhance container security including the unique seal number, the identity number of the container to which it is attached and the seal status indicator. This ISO standard (ISO Standard 18185, Freight Containers – Radio Frequency Communication Protocol for Electronic Seal) is currently in the balloting stage and is expected to become a final industry standard by December 2002. Further, the United States believes that manufacturers will be able to supply the necessary quantity of electronic seals meeting this standard by July 2004.

7 A number of the containers transported by ship are empty, therefore, consideration needs to be given as to whether or not they should be sealed. Once a container is unloaded, its movement is uncertain and it could remain idle for weeks or months in a number of locations. Current business practice when shipping empty containers is to verify that they are in fact empty at the various stops in the inter-modal transportation chain. Carriers should continue to verify that empty containers are in fact empty before accepting them for shipment. The United States recognizes that there could be business implications on requiring all empty containers to be sealed, either electronically or mechanically. This issue should be further studied in conjunction with the WCO before imposing such a requirement.

8 With all of the above in mind, the United State proposes that new regulations for container security be added to Chapter XI of SOLAS as follows (It should be noted that two options are provided for seals, one for a mechanical seal and another for an electronic seal, depending upon whether or not the ISO 18185 standard for electronic seals is adopted in time for the IMO conference in December 2002.):

Option One for electronic seals –

"The shipper shall ensure that before a loaded container is offered for shipment on board a ship, the container is sealed with an electronic seal* that records the seal's unique identification number, the container number to which it is affixed and the status of the seal.

*Reference is made to ISO Standard 18185, Freight Containers – Radio Frequency Communication Protocol for Electronic Seal."

Option Two for mechanical seals –

"The shipper shall ensure that before a loaded container is offered for shipment on board a ship, the container is sealed with a mechanical high security seal* that is uniquely numbered.

*Reference is made to American Society of Testing Materials (ASTM) Standard F832, Classification for Security Seals, Level D." NOTE: The United States is not aware of an ISO mechanical seal standard. If one does exist, it should be referenced here, in lieu of the ASTM standard.

9 In addition, the following requirement for the carrier should be added to Chapter XI of SOLAS or Part A of the Security Code, whichever is deemed more appropriate:

"Each Company Security Officer shall ensure that:

.1 before a loaded container is accepted for shipment on board their company's ship, the container is sealed and the seal number and container number to which the seal is affixed are recorded in the shipping documents; and

.2 before an empty container is accepted for shipment on board their company's ship, the container is verified to be empty."

This is not intended to require the company security officer to personally check each container, but rather to ensure that company procedures are in place to do so and are followed. In addition, a corresponding requirement should also be added to the "duties and responsibilities" of the Company Security Officer contained in Part A of the Security Code.

10 <u>Non-intrusive detection and inspection.</u> Non-Intrusive Inspection (NII) technology, such as the type used by U.S. Customs, has been deployed throughout the country and used to conduct thousands of inbound and outbound examinations resulting in hundreds of contraband seizures. These systems, in many cases, provide the capability to perform thorough examinations of cargo without having to resort to the costly, time consuming process of unloading cargo for manual searches, or intrusive examinations of conveyances by methods such as drilling and dismantling.

A mix of technologies designed to complement one another and present a layered defense to smuggling attempts is the most effective method of inspection. Deployment of NII technologies allows for augmentation of staff in an attempt to maintain an alert posture while efficiently processing legitimate passengers and trade.

The United States recommends that the issue of non-intrusive detection and inspection of containers be a subject of discussion with recommendations referred to the WCO for further development and implementation by the world's customs organizations.

11 Trusted agents and shippers. In order to create an efficient and secure processing of cross-border trade, world customs organizations, nation-states and the trade community, together, need to redefine the way cargo and conveyances transit the globe.

The United States, through the U.S. Customs Service's Trade Partnership Against Terrorism (C-TPAT), will work with foreign manufacturers, exporters, carriers, importers and other industry sectors emphasizing a seamless security conscious environment throughout the entire commercial process.
By providing a forum in which the business community and the U.S. can exchange anti-terrorism ideas, concepts and information, both the government and business community will increase the security of the entire commercial process from manufacture through transportation and importation to ultimate distribution. Through the U.S. program, C-TPAT trade partners will make a commitment to both trade security and trade compliance, which are rooted in the same business practices, to work closely with companies whose good business practices ensure supply chain security and compliance with trade laws. This program summarizes the United States efforts to develop trusted agents and shippers in the trade environment.

The United States recommends that the subject of trusted agents and shippers be a subject of discussion under the agreement with WCO and that the world's customs organizations work expeditiously to implement programs to address cargo and conveyance efficiency and security.

12 Shipper identification numbers. The use of a standardized number to identify all shippers of merchandise is considered to be an important element in the data collection portion of U.S cargo security initiatives, which are implemented in the U.S. by the U.S. Customs Service. Such a standardized number should provide information identifying the shipper (consignor, seller, exporter, manufacturer and even the factory of production) in a standardized format such as the Dun & Bradstreet Data Universal Numbering System (DUNS) number. The shipper identification number should be provided in an electronic format prior to lading. This would allow for important edits for validation of data and greater reliability in the targeting of illegally imported merchandise. Those goods improperly identified or unidentified as to shipper would be subject to more stringent controls and inspection. Conversely, shipper identification could be used as a key factor for expediting low risk merchandise from proven shippers.

The United States recommends that the subject of shipper identification numbers be a subject of discussion under the agreement with WCO. The United States further suggests that appropriate elements resulting from the discussion be further developed and implemented by either the IMO or the WCO depending upon which is the more appropriate international body for the issue at hand.

13 Cargo information in electronic format. Electronic reporting of shipment identifying data prior to the container being laden for shipment is key to securing the supply chain. The primary focus of this data is verifiable, identifying information on all of the participants in the transaction (manufacturers, shippers, carriers, importers, consignees) tied to an accurate description of the merchandise. Standardizing of Customs and other regulatory reporting data and transmission prior to lading allows for evaluation of the data by Customs in order to validate it and make examination decisions prior to the placement of the container onboard a vessel. This reduces the risk that non-legitimate interests could use the supply chain as a weapon by providing information about the shipment at the inception of the movement and using technology, following the movement to its conclusion.

The United States recommends that the subject of cargo information in electronic form be a subject of discussion and that the recommendations taken from that discussion be forwarded for further discussion and development by the WCO.

Action requested of the Committee

14 The Committee is invited to consider these proposals when discussing container security.

___